Zentralverband Deutsches Kraftfahrzeuggewerbe (ZDK)

ZDK Comments on

EDPB Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications

4th May 2020

The German Federation for Motor Trades and Repairs (ZDK) welcomes and supports the EDPB Guidelines on processing personal data in the context of connected vehicles and mobility related applications to address the concerns about personal data when communicating with the driver and the vehicle. For the mostly small- and medium-sized enterprises in the European Union the access to in-vehicle generated data and functions is essential to offer repair and maintenance services in the future.

1. About us

The German Federation for Motor Trades and Repairs represents the professional interests of more than 37.000 workshops and automotive trading companies in Germany. Our work covers the modalities of cooperation between the motor vehicle industry on the one hand and the automotive industry, the importers of motor vehicles, the employee representatives, the central associations and furthermore the legislative and regulatory bodies at national and European level on the other hand.

2. General notes

Progressive development in the automotive industry is producing vehicles able to generate, store and transmit enormous amounts of data. On the one hand, these are necessary from a technical point of view, e.g. for automated driving, but at the same time they open up the field for new vehicle-related services: Via the dashboard display it is already possible to provide drivers with a wide range of services, for example by digitally checking the condition of the vehicle and identifying the need for maintenance and repair. This option is currently reserved for vehicle manufacturers only. Independent service providers (ISP) are not given the opportunity to access vehicle-generated data and resources.

Market situation

Even today, vehicle manufacturers have started to take a more restrictive approach to data generated in the vehicle. Until now, diagnostic data have been read out of the on-board computer via an interface (OBD II) in a stationary manner - whether by the manufacturer or by an independent supplier. It is becoming increasingly apparent that vehicle manufacturers are moving towards reducing the interface to emission-relevant data and restricting the function during driving, while the number of service offers by the manufacturer's own networking solutions is increasing. This massively limits the development of innovative mobility offers in the aftermarket and restricts the competitive market.

Ensure freedom of choice for consumers and free competition

Effective competition is only possible if the vehicle user can send the vehicle-generated data to the company authorised by him and if this company also has real time on-board access to, for example, the display in the dashboard (Human-Machine-Interface). It must be ensured that vehicle manufacturers do not have exclusive data and access control. Networking in the vehicle can only be fair and reasonable for the consumer if the following criteria are met:

1. **Efficient competition between all players in the automotive sector**

   Free access to the data and customer interface in the vehicle, independent of the manufacturer, is a precondition for independent market players to develop and offer innovative and diverse telematics services at fair prices.

2. **Freedom of choice for consumers**

   Consumers do not have the option of sending the data directly to a service provider of their choice. Communication can currently only take place via the driver's smartphone, but this is forbidden while driving in the interests of road safety. This makes it more difficult for independent service providers to obtain the consent of the respective driver to use his data in a modern, consumer-friendly manner in compliance with data protection regulations.

3. **Data protection**

   The in vehicle processing and use of personal data generated by vehicles may only take place expressly if consumers have been fully informed in advance and have expressly consented to the in vehicle processing.

4. **Cyber Security**

   All communication channels within the vehicle and to the outside must be standardized according to the current security requirements and, if applicable, those still be developed. This is the only way to ensure the operational safety of environmentally relevant systems and road safety over the entire life cycle of a vehicle.

OTP ensures efficient and secure access to the vehicle

An in-vehicle, interoperable, standardised and secure telematics platform (OTP), which provides secure real time on-board access even to time-critical data and functions can stimulate innovation and productivity. This enables applications - which are developed and tested according to uniform certified development and security standards - to be executed securely in the vehicle. A third-party application is accessing data generated in the vehicle in the same way and quality as vehicle manufacturers and uses the same functions (e.g. interaction with the driver) in the vehicle for the respective service (e.g. repair service, route planning). The vehicle manufacturers and the independent service providers may only be provided with access to data if a standardized procedure is followed, with protection to both inside and outside against attacks and manipulation. The basis for this is a security architecture that creates a uniform and interoperable standard with regard to IT security in the networked vehicle itself (endpoint security) and associated smart services. That this is

technically possible is shown, for example, by a comparable platform that is already being used in the first new vehicle generations of few vehicle manufacturers.

In contrast to the access procedures offered by vehicle manufacturers via outsourced servers, the open telematics platform (OTP) offers the following advantages:

- Secure access to data is taking place directly in the vehicle.
- The data in the vehicle can be processed by using third-party applications approved by the vehicle manufacturer. Data are only sent to an external server if this is necessary to provide the service. This takes account of data economy and significantly increases security.
- Third-party applications are offered to the driver in the vehicle via customer interface and get/receive the same data used by the vehicle manufacturer.
- Direct relations between the consumer and the independent service provider (ISP).

3. Comment to Guidelines

For the mostly small- and medium-sized enterprises in the European Union the access to in-vehicle generated data and functions is indispensable to offer repair and maintenance services in the future.

The German Federation for Motor Trades and Repairs (ZDK) supports the Guidelines on processing personal data in the context of connected vehicles and mobility related applications to address the concerns about personal data when communicating with the driver and the vehicle.

2.1 Categories of data

Page 12 […] This includes technical data concerning the vehicle's movements (e.g., speed, distance travelled) as well concerning the vehicle's condition (e.g., engine coolant temperature, engine RPM, tyre pressure) […]

ZDK comment:

In our opinion, technical data concerning the vehicle's condition (e.g. engine coolant temperature) as mentioned in 2.1 required for repair and maintenance services are not direct personal data as these data are processed in a closed system and have no relationship to other data. This means that no conclusions can be drawn about a person. Access to this machine-generated data is only granted after the driver's consent.

2.3 Relevance and data minimisation

Page 14 […] To comply with the data minimization principles, vehicle and equipment manufacturers, service providers and other data controllers should pay special attention to the categories of data they need from a connected vehicle, as they shall only collect personal data that are relevant and necessary for the processing. For instance, location data are particularly intrusive and can reveal many life habits of the data subjects. Accordingly, industry participants shall be particularly vigilant

not to collect location data except if doing so is absolutely necessary for the purpose of processing (see discussion on geolocation data above, in section 2.2).

ZDK comment:

Where possible, data processed in the vehicle should only be sent to an external server if this is necessary for the provision of the service. This takes account of data economy and considerably increases security.

2.4 Data protection by design and by default

Page 14 […] Technologies should be designed to minimize the collection of personal data, provide privacy-protective default settings and ensure that data subjects are well informed and have the option to easily modify configurations associated with their personal data. Specific guidance on how manufacturers and service providers can comply with data protection by design and by default could be beneficial for the industry.

ZDK comment:

The last sentence should be amended as follows: […] Specific guidance on how manufacturers and service providers can comply with data protection through design and default settings could be beneficial for industry **and third party application providers**.

2.5 Information

General ZDK comment:

The Rules of data protection, data minimisation and privacy must also apply between third party service providers at varius levels in the value chain. For example between an independent repair workshop and the original manufacturer of the vehicle. Any type of backtracing is dependent on the users consent and must be informed to the third party and user.

2.7 Security and confidentiality

Page 20 […] implementing technical measures that enable vehicle manufacturers to rapidly patch security vulnerabilities during the entire lifespan of the vehicle;

ZDK comment:

The implementation of technical measures enabling vehicle manufacturers to rapidly close safety gaps throughout the life of the vehicle; these measures must relate exclusively to the safety architecture and not to measures necessary for the maintenance and repair of the vehicle over the air.

3.1 Provision of a service by a third party

General ZDK comment:

With the high dependency of the whole repair and maintenance industry on a continued access to in vehicle generated data and services, ZDK recommends to EDPB to including a case study looking into the details and operations of data processing and security of personal data for the purposes of remote vehicle diagnostics, repair and maintenance services. Especially the relationship between manufacturers and aftermarket.

Werner Steber Alex Jan Erdmann Dominik Lutter

German Federation for Motor Trades and Repairs (ZDK)

Franz-Lohe-Straße 21, 53129 Bonn - Germany
Phone: +49 228 9127 292
Email: technik@kfzgewerbe.de